IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

KERRON D. ANDREWS	*	**UNDER SEAL**
Plaintiff,	*	
v.	*	**Civil Case No.: SAG-16-2010**
BALTIMORE CITY POLICE DEPARTMENT, *et al.*,	*	
Defendants.	*	

* * * * * * * * * *

MEMORANDUM OPINION

This Section 1983 lawsuit arises out of the Baltimore Police Department's use of a cell-site simulator to locate Plaintiff Derron Andrews in 2014. Plaintiff alleges that Defendants Baltimore Police Department and Commissioner Kevin Davis (collectively, "BPD"),[1] and BPD Officers Michael Spinnato and John Haley (collectively, "Officer Defendants"), violated his Fourth Amendment rights[2] by using a "Hailstorm" device to locate him without a warrant. The United States Court of Appeals for the Fourth Circuit, which retains jurisdiction over this case, remanded for further factfinding about the simulator's functionality. ECF 60. Supplemental discovery has now concluded, ECF 165, 169, 170, and the Officer Defendants and BPD have filed new motions for summary judgment. ECF 184, 185. Plaintiff opposes both motions. ECF 188,

[1] Because Plaintiff has only sued Commissioner Davis in his official capacity, Plaintiff's suit against Davis is legally identical to a suit against the BPD itself. *See Kentucky v. Graham*, 473 U.S. 159, 166 (1985). This Court will accordingly consider them together. The Officer Defendants are being sued in their individual capacities.

[2] Plaintiff also alleges that Defendants violated his rights under Article 26 of the Maryland Declaration of Rights. Maryland courts interpret Article 26 *in pari materia* with the Fourth Amendment of the Constitution. *Richardson v. McGriff*, 361 Md. 437, 762 A.2d 48, 56 (2000).

189. Each group of Defendants filed a reply in support of their respective motion. ECF 195, 196. No hearing is necessary. *See* Loc. R. 105.6 (D. Md. 2023). This Court has made the factual findings and conclusions of law requested by the Fourth Circuit, and would grant Defendants' motions for summary judgment if it had jurisdiction to do so.[3]

I. BACKGROUND

The underlying facts of this lawsuit are largely undisputed and were recounted at length in the Appellate Court of Maryland's opinion from Plaintiff's criminal case. *State v. Andrews*, 277 Md. App. 350 (2016). On April 27, 2014, three people were shot during a drug deal in Baltimore City. *Id.* at 356. A witness identified Plaintiff as the shooter from a photo array, and a warrant was issued for his arrest. *Id.* Defendant Spinnato sought a Pen Register Order ("PRO") allowing BPD to use cellular device tracking to locate Plaintiff. *Id.* Judge Barry Williams of the Circuit Court for Baltimore City signed the PRO, noting that "probable cause exist[ed]." *Id.* at 357. The PRO described the phone number to be traced, set a 60-day time limit, and authorized officers "to employ surreptitious or duplication of facilities, technical devices, or equipment to accomplish the installation and use of a Pen Register\ Tap & Trade and Cellular Tracking Device" and to "initiate a signal to determine the location of the subject's mobile device." *Id.* at 356–58. It did not specifically mention a "cell-site simulator" or a "Hailstorm," and did not have geographic limits.

[3] The Fourth Circuit has presented specific issues for this Court to address, but the appeal remains pending. Given that procedural posture, although this Court will evaluate the parties' arguments under the summary judgment standard, it is this Court's understanding that it lacks jurisdiction to enter or deny summary judgment. Rather, the purpose of this opinion is to provide the Fourth Circuit with supplemental information to facilitate its evaluation of the still-pending appeal. Although the parties have focused on other issues, including immunity doctrines and whether genuine issues of material fact exist, because the Fourth Circuit has expressly requested conclusions of law regarding the substance of Plaintiff's Fourth Amendment claim, this Court will focus its attention there. This Court also will not deem any party to have waived any argument based on a failure to respond, given the unusual way these issues have been presented.

Under the PRO, BPD officers on the "Advanced Technical Team," including Defendant Haley, obtained the location of Plaintiff's phone within a 200-to-1600-meter radius. *Id.* at 359. On May 5, 2014, the Officer Defendants went to that area and Defendant Haley used a cell-site simulator, the "Hailstorm," to locate Plaintiff's cellphone at 5032 Clifton Avenue. *Id.* Defendant Spinnato knocked on the door and received consent to enter. *Id.* Plaintiff was inside with the target cellphone. *Id.* The officers arrested Plaintiff and obtained a search warrant for 5032 Clifton Avenue. *Id.*

A grand jury indicted Plaintiff on May 29, 2014. *Id.* After nearly a year of litigation related to the Defendant Officers' identification and locating of Plaintiff, the State revealed that the officers used a "stingray"-type device to locate Plaintiff's cellphone. *Id.* at 360–61. Plaintiff moved to suppress, seeking to exclude all evidence obtained from 5032 Clifton Avenue. *Id.* at 361. The Circuit Court for Baltimore City granted Plaintiff's motion to suppress, finding that Defendants' warrantless use of the Hailstorm device was an unreasonable search under the Fourth Amendment. *Id.* at 367. The Appellate Court of Maryland affirmed, holding that "the use of a cell site simulator requires a valid search warrant, or an order satisfying the constitutional requisites of a warrant, unless an established exception to the warrant requirement applies." *Id.* at 395. Plaintiff prevailed in his criminal case in June of 2016. ECF 184-1 at 3.

Shortly thereafter, Plaintiff filed this civil rights lawsuit in Baltimore City Circuit Court, and Defendants removed to this Court. ECF 1, 2. In 2018, United States District Judge Catherine C. Blake granted the Defendants' motion for summary judgment, finding that the Pen Register Order met the Constitutional requirements for a warrant, and therefore Plaintiff's Fourth Amendment rights were not violated. ECF 54 at 11–18.

The Fourth Circuit disagreed, expressing concern that the PRO did not specifically authorize or disclose the use of a cell-site simulator, and that the device may have searched cellular devices other than Plaintiff's and penetrated through walls. ECF 60 at 3–4. The Fourth Circuit found that "the record inadequately describe[d] the degree of intrusion onto constitutionally protected areas that occurred as a result of the Hailstorm simulator's use," such as "how many devices were identified," its full operational range, and "what data it collected and stored." *Id.* It accordingly remanded with instructions for this Court to conduct additional factfinding on the following issues:

> (1) The maximum range at which the Hailstorm simulator can force nearby cellular devices to connect to it.
>
> (2) The maximum number of cellular devices from which the Hailstorm simulator can force a connection
>
> (3) All categories of data the Hailstorm simulator may collect from a cellular device, regardless of whether such data is displayed to the Hailstorm simulator's operator in the course of locating a target phone, including by way of example and without limitation: cellular device identifiers (such as international mobile equipment identity ("IMEI") numbers, international mobile subscriber identity ("IMSI") numbers, and electronic serial numbers ("ESN")); metadata about cellular device operations (such as numbers dialed or texted, or webpages visited); and, most especially, the content of voice or video calls, text messages, emails, and application data.
>
> (4) What data in (3) may be stored by the Hailstorm simulator.
>
> (5) What data in (4) are accessible by law enforcement officers.
>
> (6) All means by which the Hailstorm simulator was configured to minimize data collection from third party cellular devices not belonging to Andrews.
>
> [And] whether—aside from the non-disclosure agreement between BPD and the FBI—BPD had, at the time of its application for the Pen Register Order, any formal or informal policies, practices, or procedures that prevented BPD officers seeking a warrant or pen

> register/trap and trace order from stating to the reviewing magistrate that a cell site simulator would be used.

ECF 60 at 7–8. The Fourth Circuit further instructed this Court to provide updated conclusions of law on whether the BPD's use of the Hailstorm device violated the Fourth Amendment based on the supplemented record. *Id.* at 8. At the close of discovery, Plaintiff, ECF 165, the Officer Defendants, ECF 169, and BPD, ECF 170, filed memoranda outlining their responses to the Fourth Circuit's questions.

II. FACTS ASCERTAINED FROM SUPPLEMENTAL DISCOVERY

The Court considers the facts in the light most favorable to Plaintiff as the nonmoving party.

A preliminary matter warrants discussion. Plaintiff argues that he was unable to provide definitive answers to some of the Fourth Circuit's areas of inquiry because he did not have access to a Hailstorm operator's manual. ECF 160 at 8–9; ECF 189 at 4. The corporate representative for L3Harris, the manufacturer of the Hailstorm, clarified that L3Harris does not provide an operator's manual to customers, and did not provide one to BPD. ECF 160-4 at 78–80. The operator's manual, moreover, was "not for the device used to locate Andrews or…applicable to Hailstorm used by the Baltimore City Police Department or any U.S. local law enforcement." ECF 152-2. It discussed "Hailstorm capabilities and functionality not available to any state and local law enforcement customers," and L3Harris accordingly considered it "sensitive and highly confidential." *Id.* L3Harris gave BPD a quick start guide, which was produced to Plaintiff in this case. ECF 160 at 8.

This Court denied Plaintiff's motion to compel production of the operator's manual, noting that "this case is limited to the device used by the BPD to locate…Andrews," the manual provided to BPD had already been produced, and the operator's manual was not applicable to BPD's

Hailstorm. ECF 154. This Court sees no reason to revisit those findings or to presume the operator's manual would have provided further clarity on the Fourth Circuit's questions. The parties engaged in more than three years of discovery, and Plaintiff was given a great deal of latitude in conducting discovery. Although some of the facts in this case remain unclear, this Court does not believe that there are genuine disputes over them. Rather, the specifics of the Hailstorm's operation seem to vary depending on context, and certain aspects of that context in Plaintiff's case cannot be ascertained more than ten years later.

As the parties did, this Court will begin with a brief summary of cell-site simulators in general.

1. Cell-Site Simulators

Cell-site simulators work by emulating cell-phone towers. ECF 170-8 at 23. Cell phones "are designed to seek, identify, and connect with" cell towers around them. *In re Use of a Cell-Site Simulator to Locate a Cellular Device*, 531 F. Supp. 3d 1, 4 (D.D.C. 2021). Cell phones cannot differentiate between a cell tower and a simulator operated by law enforcement. *United States v. Thorne*, 548 F. Supp. 3d 70, 114 (D.D.C. 2021). Because cell-site simulators emit a stronger signal than most cell towers, most cell phones will "identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator the identify the device in the same way that they would with a networked tower." *Id.* (quoting U.S. DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR 2 (2015)). Every phone has a unique, fifteen-digit number (called an ISMI or IMEI), that has no relation to a cell phone number. 170-8 at 44, 47. The number can only be obtained directly from a cellular provider. *Id.* at 137. When a cell phone connects to a cell tower or cell-site simulator, it transmits its unique identifier number. *Id.* at 47–48.

The cell-site simulator at issue here, the Hailstorm, works by emulating a cell tower and searching for the fifteen-digit identifier associated with the target phone. *Andrews*, 227 Md. App. at 362; ECF 170-6 at 308. To use a Hailstorm to search for a target phone, an officer would "[t]urn it on, plug in a specific, unique 15-digit identifying number that specifically identifies only that device and drive around the area that the phone company last knew that phone to be." ECF 170-8 at 43. BPD's Hailstorm was installed in a police car and connected to a laptop. ECF 170-6 at 118–19. The Hailstorm connects to devices like a cell tower. *Id.* at 156–57. [redacted]

2. Factfinding in Response to Fourth Circuit's Questions

a. The Maximum Range of the Hailstorm

The Fourth Circuit first asked this Court to conduct factfinding on the maximum range of a Hailstorm device. The parties agree that [redacted] As former BPD Lieutenant David Rosenblatt testified, the device has a fairly long range "if there's nothing in the way," but "[i]f it's on a ground level and there's block buildings and steel all around me and concrete, maybe it works ten feet." ECF 170-8 at 46. [redacted]

[redacted] Defendant Haley, who operated the Hailstorm device at issue here, estimated the device's range as one to two blocks in Baltimore City. ECF 165-5 at 24. In a hearing in Plaintiff's criminal case, Defendant Haley noted that the device does not indicate distance, but points its operator in the direction of the signal and gives a numeric indication of the strength of the signal. *Andrews*, 227 Md. App. at 364.

In sum, [redacted]

b. The Maximum Number of Devices to which a Hailstorm could Connect

[redacted] Plaintiff used Sprint.[4] Although Sprint's market share was less than 25% in 2014, *see* U.S. Wireless Carriers: 2014 in Review, Forbes (Dec. 26, 2014), this Court will conservatively estimate that the Hailstorm connected to a quarter of devices in its range. [redacted]

[4] Sprint did not merge with T-Mobile until 2018.

[redacted]

It appears, again, the maximum is a context-specific assessment, and this Court lacks some necessary context. At any rate, it appears that the device would connect to around one-quarter (assuming four main cellular providers) of phones within the small range of the device.

c. Data Collection

The Hailstorm device works by [redacted] The only information it ever collects from any phone is the electronic identifier number and [redacted]

For any device, target or not, the Hailstorm does not collect metadata, numbers dialed, the content of voice or video calls, a record of text messages or their content, a record of web pages visited, the content of emails, any application data about cellular device operations, photographs stored on phones, or any content stored on a phone. ECF 170-4; ECF 170-6; ECF 170 at 25–26. It also does not collect telephone numbers. ECF 170-8 at 47.

In sum, the Hailstorm only collects electronic identifier numbers and [redacted]

d. Data Storage

Next, this Court was tasked with assessing what collected data Hailstorms store. Hailstorms only store the electronic identifier and [redacted]

[redacted]. Defendant Haley testified that he purged Hailstorm data daily, and never backed up any data on the device or saved it elsewhere. ECF 170-4 at 28. Detective Rosenblatt, by contrast, did not know if the device had been purged and did not recall personally purging the Hailstorm. ECF 170-8 at 75.

If the device was not purged, it would only store the electronic identifier of the target device. However, it is undisputed that the BPD Hailstorm was purged by the officer who operated it daily. The Hailstorm at most stored the electronic identifier, but more than likely stored no data at all.

e. Data Accessibility

Fifth, this Court was instructed to determine what data stored in the Hailstorm could be accessed by law enforcement officers. BPD kept its Hailstorm device in a locked vehicle in a secure garage that was only accessible by a limited number of officers using both a keycard and biometric data. ECF 170-8 at 37–38. Any stored data remains on the device itself, not on a cloud or external server. ECF 165-18 at 288. If there was data stored on the device, any person with access to the device (including the device's password) could access that data. ECF 165-20 at 291. It is possible to extract data from a Hailstorm using a thumb drive. ECF 165-17 at 28–29; ECF 165-19 at 289.

This Court accordingly finds that, as most, a limited number of law enforcement officers with the requisite credentials could access the stored electronic identifier numbers of target devices. The far more likely scenario, however, is that no data at all was stored on the BPD Hailstorm because its operators purged data as they were instructed to and did not modify the default settings.

f. Device Configuration

Sixth, the Fourth Circuit requested further information regarding "[a]ll means by which the Hailstorm simulator was configured to minimize data collection from third party cellular devices not belonging to Andrews." ECF 60 at 8. As described above, a Hailstorm [redacted] only interacts with [redacted] only ever collects fifteen-digit identifier numbers, [redacted]. And the identifier numbers cannot be tied to the owner of the phones, any of their personal information, or even any information about the phones, without subpoenaing the provider. ECF 170-6 at 301–03.

There is no record evidence suggesting BPD's Hailstorm was reconfigured from default mode. And even if someone did reconfigure the device, the record reflects [redacted] It does not appear to the Court that BPD's Hailstorm was configured in any special way to avoid collecting third-party data, but rather that the Hailstorm, whether in default mode or not, is designed to find the target phone, not to collect data from other phones.

g. BPD Policies, Practices, and Procedures

Finally, the Fourth Circuit asked this Court to assess whether—apart from a non-disclosure agreement between BPD and the Federal Bureau of Investigations ("FBI")—BPD had "any formal or informal policies, practices, or procedures that prevented BPD officers seeking a warrant or pen register/trap and trace order from stating to the reviewing magistrate that a cell site simulator would be used." ECF 60 at 8.

BPD and the Officer Defendants (who applied for the PRO) deny the existence of any policy preventing them from disclosing the use of a cell-site simulator in a pen register order or warrant application. ECF 169 at 3–4; ECF 170 at 30–31. Defendant Haley, who applied for the PRO, believes he would have been permitted to disclose the use of a Hailstorm in applying for a PRO. ECF 170-4 at 56. Further, Defendants argue that "the [c]ourt is informed of the use of a cell site simulator when it reviews and signs the Pen Register Application and Order because the order indicates a 'cellular tracking device' will be used." ECF 170 at 31 (citations omitted). James Green, former Deputy Chief Legal Counsel for BPD, testified that "cellular tracking device is a synonym for cell-site simulator." ECF 170-10 at 82; *see also* ECF 170-8 at 165–66 (former BPD ATT commander affirming that the terms were used interchangeably).

Plaintiff continues to rely on the non-disclosure agreement BPD signed with the FBI, which Plaintiff believes would have prevented BPD from naming the Hailstorm to the issuing magistrate and "goes to the policies implemented by the police department." ECF 189 at 9–10. Plaintiff did not identify any particular BPD policy apart from the NDA. The NDA required BPD to obtain written permission to disclose its use of the Hailstorm in any civil or criminal proceeding. *See Andrews*, 277 Md. App. at 374–75.

III. LEGAL STANDARD

Under Rule 56(a) of the Federal Rules of Civil Procedure, summary judgment is appropriate only "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." The moving party bears the burden of showing that there is no genuine dispute of material fact. *See Casey v. Geek Squad Subsidiary Best Buy Stores, L.P.*, 823 F. Supp. 2d 334, 348 (D. Md. 2011) (citing *Pulliam Inv. Co. v. Cameo Props.*, 810 F.2d 1282, 1286 (4th Cir. 1987)). If the moving party establishes that no evidence supports the non-moving party's case, the burden then shifts to the non-moving party to proffer specific facts to show a genuine issue exists for trial. *Id.* The non-moving party must provide enough admissible evidence to "carry the burden of proof in [its] claim at trial." *Id.* at 349 (quoting *Mitchell v. Data Gen. Corp.*, 12 F.3d 1310, 1315–16 (4th Cir. 1993)). The mere existence of a scintilla of evidence in support of the non-moving party's position will be insufficient; there must be evidence on which the jury could reasonably find in its favor. *Id.* at 348 (citing *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 251 (1986)). Moreover, a genuine issue of material fact cannot rest on "mere speculation, or building one inference upon another." *Id.* at 349 (quoting *Miskin v. Baxter Healthcare Corp.*, 107 F. Supp. 2d 669, 671 (D. Md. 1999)).

Additionally, summary judgment shall be warranted if the non-moving party fails to provide evidence that establishes an essential element of the case. *Id.* at 352. The non-moving party "must produce competent evidence on each element of [its] claim." *Id.* at 348–49 (quoting *Miskin*, 107 F. Supp. 2d at 671). If the non-moving party fails to do so, "there can be no genuine issue as to any material fact," because the failure to prove an essential element of the case "necessarily renders all other facts immaterial." *Id.* at 352 (quoting *Celotex Corp. v. Catrett*, 477 U.S. 317, 322–23 (1986); *Coleman v. United States*, 369 F. App'x 459, 461 (4th Cir. 2010)

(unpublished)). In ruling on a motion for summary judgment, a court must view all the facts, including reasonable inferences to be drawn from them, "in the light most favorable to the party opposing the motion." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587–88 (1986) (quoting *United States v. Diebold, Inc.*, 369 U.S. 654, 655 (1962)).

IV. UPDATED CONCLUSIONS OF LAW

1. Fourth Amendment Claim

To evaluate whether Plaintiff's Fourth Amendment rights were violated requires a three-step inquiry: first, whether there was a search; second, whether that search was in fact warrantless; and third, whether that search was reasonable.

a. *Search*

The Fourth Circuit has already found, and the parties seem to agree, that "the Hailstorm simulator searched, at minimum, [Plaintiff's] phone, and that its use required a warrant." ECF 60 at 3. This Court does not find any reason in the updated record to revisit this finding. Nevertheless, because this is an issue of first impression, and the Fourth Circuit has expressed an interest in exploring the constitutional consequences of Hailstorm use with more information on its function, this Court will define the contours of the search at issue.

"[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 553 U.S. 27, 33 (2001). "[I]individuals have a reasonable expectation of privacy in the whole of their physical movements." *Carpenter v. United States*, 585 U.S. 296, 310 (2018). With this in mind, the Supreme Court has found that "government access to cell-site records contravenes that expectation." *Id.* at 311. But this Court is cognizant that the privacy concerns associated with real-time tracking are less serious than those associated with long-term historical tracking. *See id.* (127

days of "time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"); *id.* at 312 (discussing risks posed by "retrospective quality" of surveillance). A one-time ping does not pose the same risks of intrusion as long-term surveillance.

It is true, however, that a Hailstorm-type device can "generate a precise location" for a target device, whereas longer-term cell-site information is far less precise. *United States v. Thorne*, 548 F. Sup. 3d 70, 115 (D.D.C. 2021) (quoting Carrie Leonetti, *A Hailstorm of Uncertainty: The Constitutional Quandary of Cell-Site Simulators*, 85 U. Cin. L. Rev. 665, 668 (2017)). Another key difference is that a Hailstorm-type device will have some, albeit very minimal, contact with non-target devices, whereas the kind of tracking contemplated by *Carpenter* poses no risk to third parties. Both types of tracking are capable of the kind of "through-the-wall surveillance" that could allow law enforcement to discover information "that would previously have been unknowable without physical intrusion." *Kyllo*, 533 U.S. at 40.

This Court thus agrees with Judge Blake's earlier ruling that the Hailstorm conducted a search of Plaintiff when it pinged his cell phone, made contact with it, and used that contact to locate Plaintiff's phone and Plaintiff himself. As some courts have described it, the cell-site simulator converted Plaintiff's phone into a tracking device. *United States v. Lambis*, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016). Like a thermal imaging device, the simulator allowed law enforcement to ascertain information about a private residence that was not "readily available…without the use of a cell-site simulator." *Id.* at 610 (quoting *United States v. Knotts*, 460 U.S. 276, 281 (1983)). This Court thus agrees with the courts that have found that the use of a cell-site simulator "constitutes a Fourth Amendment search within the contemplation of *Kyllo*" and thus that law enforcement was required to obtain a warrant. *Id.* at 611; *see also, e.g.*, *United*

States v. Ellis, 270 F. Supp 2d 1134, 1146 (N.D. Cal. 2017); *State v. Andrews*, 227 Md. App. 350 (2016). Using a person's cellphone as a real-time tracking device violates a reasonable expectation of privacy.

But this Court does not believe any third parties were searched. It is undisputed that the [redacted], it would be impossible for law enforcement to ascertain anything about those devices or the people who own them. [redacted] and law enforcement cannot tie that number to any phone or person without subpoenaing the cellular provider. [redacted], so there is no chance of law enforcement even attempting such a subpoena. It is unclear to this Court what expectation of privacy an individual could have in avoiding this type of inconsequential intrusion. Indeed, it appears to this Court that for third parties, the Hailstorm is *less* invasive than ordinary cell towers, which actually store and record data more easily linkable to a person's phone.

Nevertheless, this Court finds that the use of a Hailstorm to track an individual in real time is a search for which a warrant is required.

b. *Warrant*

The next question is whether the PRO constituted a warrant. A warrant must be "issued by [a] neutral and detached magistrate[]," "those seeking the warrant must demonstrate to the magistrate their probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense," and the warrant "must particularly described

the things to be seized, as well as the place to be searched." *Dalia v. United States*, 441 U.S. 238, 255 (1979).

In Judge Blake's previous opinion, this Court found that the PRO met the constitutional requirements of a warrant. ECF 54 at 16–17. In relevant part, she noted that the issuing judge made an express finding of probable cause to support the requested search. ECF 54 at 13–14. Supplemental discovery has not altered this Court's view of the first two factors (presentment and probable cause), but this Court will revisit the particularity issue with the benefit of more information about the Hailstorm.

"Unlike the probable cause requirement, which concerns the showing made by an officer seeking a search warrant, the particularity requirement is focused as well on the officer executing a warrant, and ensures that the search 'will be carefully tailored to its justifications' rather than becoming a 'wide ranging exploratory search[ ]' of the kind the 'Framers intended to prohibit.'" *United States v. Blakeney*, 949 F.3d 851, 861 (4th Cir. 2020) (quoting *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)). The Fourth Circuit has instructed district courts to "construe search warrants in a commonsense and realistic manner, avoiding a hypertechnical reading of their terms." *Id.* at 862 (cleaned up). The test "for the necessary particularity if a pragmatic one" and "[t]he degree of specificity required…may necessarily vary according to the circumstances and type of items involved." *United States v. Cobb*, 970 F.3d 319, 327 (quoting *United States v. Jacob*, 657 F.2d 49, 52 (4th Cir. 1981)).

The Constitution does not require search warrants to include "a specification of the precise manner in which they are to be executed." *Dalia*, 441 U.S. at 257. In this Circuit, "a warrant may satisfy the particularity requirement either by identifying the items to be seized by reference to a suspected criminal offense or by describing them in a manner that allows an executing officer to

know precisely what he has been authorized to search for and seize." *Blakeney*, 949 F.3d at 863. "[T]he Fourth Amendment generally leaves it to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant." *Cybernet, LLC v. David*, 954 F.3d 162, 168 (4th Cir. 2020) (cleaned up).

The PRO authorized BPD "to employ surreptitious or duplication of facilities, technical devices or equipment to accomplish the installation and use of a Pen Register \ Tap & Trace and Cellular Tracking Device" and to "initiate a signal to determine the location of the subject's mobile device on the service provider's network or with such other reference points as may be reasonably available, including a 'Real Time Tracking Tool.'" The question here is whether the PRO fairly encompassed the use of a cell-site simulator, given the functional capabilities of the Hailstorm.

Plaintiff argues that the PRO "did not provide sufficient detail" and failed "to sufficiently describe how the [cell-site simulator] device worked and what its limitations were." ECF 188 at 15. Relying primarily on *Tutis v. United States*, Plaintiff believes the PRO should have described "what [the cell-site simulator] would do in terms of receiving electronic signals from cell phone in all directions, and what it would not do in terms of not intercepting communications on such phones." 216 F. Supp. 3d 467, 479 (D.N.J. 2016). This Court disagrees with Plaintiff's reading of *Tutis*. The Government in *Tutis* was unaware of the defendant's current cell phone number or location (and believed the defendant to switch cell phones frequently), and thus sought to collect information on *every* mobile device in "close proximity" to several of the defendant's known locations. *Id.* at 472. The warrant authorized round-the-clock data collection for a month. *Id.* The District of New Jersey upheld that very broad use of a cell-site simulator in part because the warrant described the data it would and would not collect from third-party devices. *Id.* at 479. Even in that case, however, "it was not necessary for the Government to include a detailed description

in the [warrant] of how the CSS technology worked." *Id.* "The purpose of using the CSS" in that case, was to obtain electronic identifier numbers and attempt to link them to the defendant. *Id.* at 479–80.

The purpose in this case was different, and much more particularized.[5] The issuing magistrate specifically authorized BPD to use "real time tracking" and "cellular tracking" "to determine the location of the subject's mobile device." The Hailstorm used real-time tracking of Plaintiff's cell phone to locate him. It would have been better, to be clear, if BPD had expressly asked to use a Hailstorm or, at least, a cell-site simulator. *See id.* at 479. But BPD asked for and obtained permission to use an unnamed "Cellular Tracking Device" to track Plaintiff's cell phone in real time. It is not apparent to the Court that any device other than a cell-site simulator would have accomplished the same task. More than one witness testified, moreover, that "cellular tracking device" and "cell-site simulator" are synonyms. Because the PRO only sought permission to use the tracking device to determine the location of the Plaintiff's phone, it did not need to expressly disclaim the sorts of information it would never collect.

This Court accordingly believes that the PRO was sufficiently particular in defining the type of search to be performed. This was not a "general warrant." By the time law enforcement arrived at the decision to request permission use the Hailstorm, they had identified a suspect and had endeavored to locate him by conventional means. This is not a case where law enforcement indiscriminately searched large areas, but rather one where they had specific authorization to use

[5] This Court disagrees with the *Tutis* court's implication that real-time tracking is more invasive than the broad surveying of neighborhoods that occurred there. The search in the case of real-time tracking is much more targeted, better protecting the privacy interests of third parties. The PRO (or warrant) in this case, moreover, specified that this sort of cellular tracking would be used.

specific means to locate a specific person. The issuing magistrate was aware of all of these facts, and signed the PRO understanding what its purpose was.

This Court thus continues to believe the PRO constituted a valid warrant. That is not to say it was advisable for law enforcement to obtain a PRO rather than a traditional search warrant in this case, or that this Court encourages round-about descriptions of the technology the government plans to use to execute a search.[6] But, to be clear, the now-robust record in this case does not provide any evidence to support Plaintiff's theory that law enforcement was dishonest or intentionally concealed information from the issuing judge before the judge made his probable cause finding.

c. *Reasonableness*

A warranted search can nevertheless be unreasonable if it is executed in an unreasonable manner. *See Cybernet LLC v.* David, 954 F.3d 162, 168 (4th Cir. 2020). In cases like this one, "significant governmental interests and significant privacy interests" are at stake. ECF 60 at 10 (Wilkinson, J., concurring). This Court must endeavor to strike the right "balance between the public interest and the individual's right to personal security free from arbitrary interference by law officers." *Pennsylvania v. Mimms*, 434 U.S. 106, 109 (1997).

The governmental interest underlying its use of the Hailstorm was no doubt significant—BPD used the Hailstorm to locate a murder suspect who had evaded capture. But even with legitimate justification, courts must ensure that "no greater invasion of privacy was permitted than was necessary under the circumstances." *Katz v. United States*, 389 U.S. 347, 355–56 (1967).

---

[6] This Court is aware that there are federal and state law-enforcement reasons not to disclose certain highly specific information, such as the name of the device to be used or its precise capabilities. Nevertheless, the government should endeavor to be as transparent as possible while protecting critical law enforcement details.

Plaintiff's privacy interests here were significant too—he was in a private residence, and the government used his cell phone to track him. As the Supreme Court has recognized, there are unique privacy interests associated with cell phones, which store "a digital record of nearly every aspect of…li[fe]—from the mundane to the intimate." *Riley v. California*, 573 U.S. 373, (2014). But this is not a case about searching the contents of a phone. In a variety of contexts, courts have found GPS tracking—even for somewhat extended periods of time—appropriate. *See, e.g.*, *United States v. Jones*, 565 U.S. 400, 404 (2012).

Actions by officers acting pursuant to a valid search warrant are presumed to be reasonable. *Anglin v. Dir. of Patuxent Inst.*, 439 F.2d 1342, 1346 (4th Cir. 1971). This Court agrees with BPD that the "brief interaction" between the Hailstorm and Plaintiff's phone was "proportionate to the need to locate a specific target…in this case involving an individual wanted for attempted murder." ECF 185-1 at 7–8. The Hailstorm collects no data from third parties, and only very minimal data from a targeted person. The officers in this case were judicially authorized to use "cellular tracking" to locate Plaintiff. They did not collect any information unnecessary to accomplish that task, and they did not use the Hailstorm for any reason other than locating Plaintiff. The officers did not sit on any data or put any data at risk of improper disclosure. They did not search anyone or any place they were not authorized to search. In sum, they stayed well within the bounds of the warrant. Using the "common sense" approach proscribed by the Fourth Circuit, this Court believes the warrant was executed in a reasonable manner. *See United States v. Srivastava*, 540 F.3d 277, 289 (4th Cir. 2008). The Fourth Amendment protects only "against intrusions which are not justified by the circumstances, or which are made in an improper manner." *Maryland v. King*, 569 U.S. 435, 447 (2013) (quoting *Schmerber v. California*, 384 U.S. 757, 768 (1966)). The intrusion here was both justified by the circumstances and made in a proper manner.

* * *

Because this Court would find that there was no constitutional violation in this case, it need not address qualified immunity, public official immunity, or *Monell* liability. In a different procedural posture, however, this Court would have granted summary judgment without reaching the constitutional question because no clearly established law barred the Officer Defendants' conduct in 2014, so they are entitled to qualified immunity. Indeed, the law on this issue is not clear even today. Additionally, the officers were acting within the scope of their employment, warranting public official immunity, and discovery in this case has revealed no official policy or custom that would justify *Monell* liability.

V. CONCLUSION

As the Court of Appeals has retained jurisdiction over this matter, this Court will issue an indicative ruling under Fed. R. App. P. 12.1 and Fed. R. Civ. P. 62.1. If this Court had jurisdiction to do so, it would grant both motions for summary judgment because there is no genuine issue of material fact as to whether the Defendants violated Plaintiff's constitutional rights.

The parties must promptly notify the Clerk of Court for the United States Court of Appeals for the Fourth Circuit of this Court's opinion. This Court is filing this memorandum opinion under seal, and the parties are ordered to provide this Court with proposed redactions no later than one week after the date of this opinion so that it may be filed on the public record.

Dated: March 4, 2025

/s/
Stephanie A. Gallagher
United States District Judge